



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/746,393	12/21/2000	John E. Schier	062891.0491	3364

7590 06/22/2004
Kevin J. Meek, Esq.
Baker Botts L.L.P.
2001 Ross Avenue
Dallas, TX 75201

EXAMINER

HUA, LY

ART UNIT PAPER NUMBER

2135

DATE MAILED: 06/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/746,393

Applicant(s)

SCHIER, JOHN E.

Examiner

Ly V. Hua

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-11 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-11 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date ____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: ____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:
The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.
2. Claims 121 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

a. With regard to claim 1:

- i. It is not clear as to what is being modified by the phrase "using an encryption table stored at the transmitting device."

(1) Notice that it is not clear whether the phrase is used:

- (a) to modify the initial encryption algorithm or
- (b) to elaborate the purpose for which the initial encryption algorithm is to be selected or
- (c) to indicate how the encryption selection key value is used.

- ii. The body of the claim does not support the preamble.

(1) Notice that:

- (a) the preamble is set forth to claim a method of communicating "voice transmissions" but the body of the claim does not clearly recite any step wherein the "voice transmissions" is communicated.
- (b) the "information associated with the voice transmissions" itself does not appear to be the "voice transmissions" (since for example, the associated information could be the addresses of both of the transmitter and the receiver).

iii. The phrase "the encryption key value" (in the clause reciting the using step) lacks antecedent basis.

iv. It is not clear as to how the state of being of the encryption key value is brought forth by a step of the method (if any) or how it affects the method.

v. It is not clear as to how the state of being of the transmitting device affects the steps being recited or affected by those steps.

vi. The words "information" and "associated" in phrase "information associated with the voice transmissions" are vague as they are recited in the claim.

vii. The phrase "in an encrypted form" (recited in the transmitting step) is confusing.

(1) Notice that:

- (a) it is not clear whether the phrase is:

(i) to modify the information associated with the voice transmissions or

(ii) to modify the voice transmission itself; and

- (b) if the phrase is to modify the information associated with the voice transmission, then it is not clear as to whence such information is encrypted.

b. With regard to claim 2:

- i. The term "the encryption key value" referring to the phrase "the encryption key value" (in claim 1) which lacks antecedent basis, and thus itself also lacks proper antecedent basis.

c. With regard to claim 3:

i. The term "the key value" lacks proper antecedent basis.

- (1) Notice that up to this point in claim 3 itself and in its parent claims 1 and 2, more than one key value have been recited (including "an encryption selection key value", "a periodic key value", "a public variable key value").

d. With regard to claim 4:

- i. In the recitation of step of "transmitting data associated with the voice communication using the next encryption method," (1) it is not clear whether the phrase "using the next encryption method" is to modify:

- (a) the transmitting,
- (b) the data or
- (c) the voice communication.

e. With regard to claim 5:

- i. This claim depends on claims 1 and 4 and thus inherits the problems of indefiniteness there from.

f. With regard to claim 6:

- i. It is not clear how the tone signal is used by the receiving device.

g. With regard to claim 7:

- i. The encryption selection table is not connected to any other component and have no interaction with any of those components.
 - ii. It is not clear as to how the CPU's ability to interact with a user affects the method or affected by the method.
 - iii. The body of the claim does not support the preamble.
- (1) Notice that the preamble is set forth to claim a telecommunications device to send and receive encrypted voice communications through a public switched telephone network, but the body of the claim does not clearly recite any limitation indicating that the device is communicating through such public switched telephone network.

h. With regard to claim 8:

- i. The phrase "the indicated key value" lacks antecedent basis.
- ii. Claim 8 depends on claim 7 but it does not further limit the device of claim 7 since the wherein clause is referring to the "indicated key value" that has not been recited in claim 7.

i. With regard to claims 9 and 10:

- i. These claims depend on claim 7, and thus inherit the problems of indefiniteness there from.

j. With regard to claim 11:

- i. This claim does not further limit claim 9 upon which it depends. Notice that it just repeats the texts that have been recited in its parent claim 9.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:
A person shall be entitled to a patent unless –
(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1, 4, 5 and 7-11 are rejected under 35 U.S.C. 102(b) as being anticipated by Wilson (5,185,796).

<p>k. Applicant's claim 1 claims a method of communicating</p> <p>i. (1) voice transmissions to a receiving device from a transmitting device,</p> <p>ii. comprising:</p> <p>(1) using</p> <p>(a) an encryption selection key value to select</p> <p>1) an initial encryption algorithm using an encryption selection table</p> <p>i) stored at the transmitting device,</p> <p>(ii) the encryption key value being</p> <p>1) a function of at least one or both of</p> <p>a) a periodic key value and</p> <p>b) a public variable key value;</p> <p>(2) encrypting</p> <p>(a) the initial voice transmissions from the transmitting device,</p> <p>1) the transmitting device being capable of encrypting</p> <p>a) voice transmissions using a plurality of encryption methods</p> <p>(b) using the initial encryption algorithm; and</p> <p>(3) transmitting</p> <p>(a) information associated with the voice transmissions in an encrypted form from the transmitting device.</p>	<p>l. As per claim 1, Wilson teaches a method of communicating</p> <p>i. (1) voice transmissions to a receiving device [200] from a transmitting device [100],</p> <p>ii. comprising:</p> <p>(1) using</p> <p>(a) an encryption selection key value [409] to select [see "selection of algorithm and key" in Wilson's Detailed Description Text, paragraph 24]</p> <p>1) an initial encryption algorithm</p> <p>a) using an encryption selection table [108]</p> <p>i) stored at the transmitting device [100],</p> <p>(ii) the encryption key value [403, i.e., the input (other than the plain text) to the encrypting element 402] being</p> <p>1) a function of at least one or both of</p> <p>a) a periodic key value [405] and</p> <p>b) a public variable key value [408];</p> <p>(2) encrypting [by element 402]</p> <p>(a) the initial voice transmissions [401] from the transmitting device [100],</p> <p>1) the transmitting device being capable of encrypting</p> <p>a) voice transmissions [401] using a plurality of encryption methods [407]</p> <p>(b) using the initial encryption algorithm [i.e., an encryption algorithm selected from among algorithms in element 407]; and</p> <p>(3) transmitting</p> <p>(a) information [i.e., the KEY ID, and the ESYNCH] associated with the voice transmissions in an encrypted form [i.e., CIPHER TEXT] from the transmitting device [100].</p>
--	--

<p>m. Applicant's claim 7 claims a telecommunications device operable to send and receive</p> <p>i. (1) encrypted voice communications through a public switched telephone network,</p> <p>ii. the device comprising:</p> <p>(1) a central processing unit</p> <p>(a) operable to interact</p> <p>(i) with a user of the device</p> <p>(ii) through a user interface;</p> <p>(2) an encryption decryption engine</p> <p>(a) operable to execute</p> <p>(i) a plurality of encryption methods</p> <p>1) under the control</p> <p>a) of the central processing unit;</p> <p>(3) an encryption selection table</p> <p>(a) accessible using an encryption key value,</p> <p>(b) the encryption selection table specifying</p> <p>(i) at least one encryption algorithm</p> <p>1) associated with each of the encryption key values; and</p> <p>(4) the device</p> <p>(a) operable to encrypt</p> <p>(i) voice communications</p> <p>1) transmitted from the device</p> <p>(ii) using</p> <p>1) an initial encryption method</p> <p>a) associated with an indicated encryption key value</p> <p>key value.</p>	<p>n. As per claim 7, Wilson teaches a telecommunications device [i.e., either Figure 4 or 5] operable to send and receive</p> <p>i. (1) encrypted voice communications through a public switched telephone network,</p> <p>ii. the device comprising:</p> <p>(1) a central processing unit [inherent in host computer 102]</p> <p>(a) operable to interact</p> <p>(i) with a user of the device</p> <p>(ii) through a user interface [that is inherent since a computer is to have interface (such as a keyboard, a monitor, a mouse) so as to enable a user to interface with it];</p> <p>(2) an encryption decryption engine [105]</p> <p>(a) operable to execute</p> <p>(i) a plurality of encryption methods [407]</p> <p>1) under the control [see col. 2, lines 54-58]</p> <p>a) of the central processing unit [102];</p> <p>(3) an encryption selection table [108]</p> <p>(a) accessible using an encryption key value [409 (or 410)],</p> <p>(b) the encryption selection table specifying [as shown in Figure 4] at least one encryption algorithm [A, B, C]</p> <p>(i) 1) associated with each of the encryption key values [409 (or 410)]; and</p> <p>(4) the device</p> <p>(a) operable to encrypt [by using element 402]</p> <p>(i) voice communications [401]</p> <p>1) transmitted from the device [or more specifically from the device's microphone 101 through A/D converter 103 to the DSP 105]</p> <p>(ii) using</p> <p>1) an initial encryption method</p> <p>a) associated with an indicated encryption key value [see col. 3, line 59 to col. 5, line 8, for initial vector data for encryption synchronization, and the initial encryption process which is initially derived from a specially stored vector called the initialization vector (IV)].</p>
---	---

<p>o. 4. The method of Claim 1 and further comprising</p> <p>i. periodically changing</p> <p>(1) to a next encryption method</p> <p>(2) as indicated in the encryption selection table;</p> <p>(3) (Claim 5) The method of Claim 4 wherein the step of periodically changing comprises the step of changing to the next encryption method responsive to the expiration of a timer.</p> <p>ii. transmitting</p> <p>(1) data</p> <p>(a) associated with the voice communication using the next encryption method</p> <p>(2) to the receiving device; and</p> <p>transmitting</p> <p>(1) to the receiving device</p> <p>(2) a warning switch signal</p> <p>(a) (Claim 6) The method of Claim 4 wherein the warning switch signal comprises a predetermined tone detectable by the receiving device.</p> <p>(3) prior to transmitting</p> <p>(a) the data</p> <p>(i) associated with</p> <p>1) the voice communication</p> <p>a) which is encrypted using the next encryption method.</p>	<p>p. As per claim 4:</p> <p>i. Wilson teaches:</p> <p>(1) that his method comprises:</p> <p>(a) changing [according to selection of logical ID 1, 2 or 3, in element 409]</p> <p>(i) to a next encryption method [A, B or C, depending on Logical ID 1, 2 or 3]</p> <p>(ii) as indicated</p> <p>1) in the encryption selection table [108];</p> <p>(b) transmitting</p> <p>(i) data [CIPHER TEXT and ESYNC]</p> <p>1) associated</p> <p>a) with the voice communication [from element 402 to element 421]</p> <p>i) using the next encryption method</p> <p>(ii) to the receiving device [200]; and</p> <p>transmitting</p> <p>(c) (i) to the receiving device [200]</p> <p>(ii) a warning switching signal [LOGIC ID]</p> <p>(iii) (relative in time to the transmitting of the data).</p> <p>q. As per claim 5:</p> <p>i. It is understood that Wilson's method of encrypting changes responsive to the expiration of a timer since Wilson's method depends on a feedback from element 403 to element 405 for operations that are subsequent to his initial mode.</p>
---	--

<p>r. 8. The device of Claim 7 wherein the indicated key value comprises</p> <p>i. a number which is a function of</p> <p>(1) a periodic key value,</p> <p>(a) the periodic key value being a number which is agreed upon between</p> <p>(i) a transmitting party and</p> <p>1) a receiving party exchanging voice communications, and</p> <p>2) a public variable key value,</p> <p>(?) the public variable key value being a numeric value which is accessible by both</p> <p>(i) the transmitting and</p> <p>1) receiving party.</p> <p>2)</p>	<p>s. As per claim 8:</p> <p>i. Wilson shows that the key value which is being used for encrypting his data 401 is a function of:</p> <p>(1) a value [409]</p> <p>(a) that is agreed upon between</p> <p>(i) 1) his transmitting device [100] and</p> <p>2) his receiving device [200] and</p> <p>(b) a variable value [408 or 426] accessible by both of his</p> <p>(i) transmitting device [100] and</p> <p>(ii) receiving device [200].</p>
---	--

<p>t. Claim 11 just repeats reciting the limitation already recited in claim 9.</p> <p>u. Claim 9 claims that the device of Claim 7 and</p> <p>i. further comprising</p> <p>ii. (1) a timer operable to communicate with the central processing unit, the device operable to switch</p> <p>(1) to a next encryption method</p> <p>(2) (a) as indicated in the encryption selection table</p> <p>(b) by</p> <p>(a) incrementing the key value and</p> <p>(b) retrieving the next encryption algorithm</p> <p>iii. (i) associated with the incremented key value, the device operable to switch</p> <p>(1) to the next encryption algorithm</p> <p>(2) upon a signal</p> <p>(a) received by the central processing unit</p> <p>(b) from the timer</p> <p>(3) such that the device is operable to periodically change</p> <p>(a) from one of the plurality of encryption methods</p> <p>(b) to a different encryption method</p> <p>(c) during the course of a single voice communication session.</p> <p>v. Claim 11 claims that the device of Claim 9 wherein</p> <p>i. the device is operable to switch</p> <p>(1) to a next encryption method</p> <p>(2) (a) as indicated in the encryption selection table</p> <p>by</p> <p>(a) incrementing the key value and</p> <p>(b) retrieving the next encryption algorithm</p> <p>(i) associated with the incremented key value</p> <p>(3) such that the device is operable to periodically change</p> <p>(a) from one of the plurality of encryption methods</p> <p>(b) to a different encryption method</p> <p>(c) during the course of a single voice communication session.</p>	<p>w. As per claims 9 and 11:</p> <p>i. Wilson teaches:</p> <p>(1) a timer [inherent in order to produce a time of 260 milliseconds (see col. 4, line 5)] operable to communicate with his CPU,</p> <p>(2) that his device operable to switch</p> <p>(a) as indicated in the encryption selection table [108]</p> <p>(b) by</p> <p>(i) incrementing the key value [1, 2, 3 in element 409] and</p> <p>(ii) retrieving [from element 407] the next encryption algorithm [A, B or C]</p> <p>1) associated with the next incremented key value [409, (1, 2 or 3)].</p>
---	---

<p>x. Claim 10 claims that the device of Claim 9 wherein the device</p> <p>i. is further operable to transmit</p> <p>(1) a warning switch signal</p> <p>(2) to the receiving device</p> <p>(3) prior to transmitting information encrypted using the next encryption method.</p>	<p>y. As per claim 10:</p> <p>i. Wilson teaches (see Figure 3A, Col. 3, line 12 to col. 4, line 16) that his device [100] sends</p> <p>(1) warning signal [i.e., the information in the preamble] to the receiving device [200] prior to transmitting</p> <p>(c) (i) information [i.e., the output from element 402] encrypted using</p> <p>1) a) the next encryption method [i.e., subsequent to the initial encryption method using feed back key mode].</p>
--	--

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:
- (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.
6. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:
- Determining the scope and contents of the prior art.
 - Ascertaining the differences between the prior art and the claims at issue.
 - Resolving the level of ordinary skill in the pertinent art.
 - Considering objective evidence present in the application indicating obviousness or nonobviousness.
7. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wilson ('796).
- a. As per claim 6:
- Because it is not clear how the tone is to be used by the receiving device, other than just a signal that is being sent to the receiving device, the examiner equates that the claimed tone with the Logic firm as long as the energy in the signal being sent to dissipated, and still available for such conversion.
 - It would have been obvious to a person having ordinary skill in the art to realize that Wilson's signal can be sent in "tone" form.

Examiner's Comments:

2. Claims 2 and 3 have limitations that are not taught or suggested by the prior art of record.

<p>z. Claim 2 claim that the method of Claim 1 and further comprising:</p> <ul style="list-style-type: none"> i. receiving <ul style="list-style-type: none"> (1) a periodic key value at the transmitting device; ii. receiving <ul style="list-style-type: none"> (1) a public variable key value at the transmitting device; iii. calculating <ul style="list-style-type: none"> (1) an index value as a function of <ul style="list-style-type: none"> (i) the periodic key value and (ii) the public variable key value; and iv. calculating <ul style="list-style-type: none"> (1) the encryption key value as a function of the index value. (Claim 3) The method of Claim 2 wherein the key value is an integer equal to the units place of the index value. 	<p>aa. As per claim 2:</p> <ul style="list-style-type: none"> i. Wilson teaches: <ul style="list-style-type: none"> (1) that his transmitter [100] receives <ul style="list-style-type: none"> (i) periodic key value [405 that is agreed (notice that input 405 is also used by both parties) upon by both transmitting device (100) and receiving device (200)] and variable key value [408]; (ii) calculating [by element 404 in accordance with information from a value [403] <ul style="list-style-type: none"> 1) as a function of <ul style="list-style-type: none"> a) value 405 and b) value 408. ii. However Wilson does not explicitly teach: <ul style="list-style-type: none"> (1) further using the value [403] to calculate an encryption key value, (2) since Wilson uses the value [404] to do encryption, without putting further manipulation on it. iii. The prior art of record also fail to teach or suggest <ul style="list-style-type: none"> (1) deriving <ul style="list-style-type: none"> (a) an encryption key value (i) as a function of an index value, <ul style="list-style-type: none"> 1) which index value has calculated as a function of <ul style="list-style-type: none"> a) a periodic key value and b) a public variable key value.
---	---

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ly V. Hua whose telephone number is (703) 305-9684. The examiner can normally be reached on Monday to Friday from 9:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Vu Kim, can be reached on 703-305-4303. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Ly V. Hua
Primary Examiner
Art Unit 2135